地方独立行政法人　東京都立産業技術研究センター

情報セキュリティ規程

目次

第１章　総則

（目的）

第１条　この規程は、情報保護のための基本方針（情報セキュリティポリシー）（１８産技経経第４２号）（以下、「情報セキュリティ基本方針」という）に基づき、地方独立行政法人東京都立産業技術研究センター（以下、「産技研」という。）が情報セキュリティを確保することにより、業務を継続的かつ効率的に遂行すること及び社会的信頼を獲得し、保持することを目的とする。

（定義）

第２条　この規程において、次の各号に掲げる用語の意義は、それぞれ当該各号に定めるところによる。

一　「役職員」とは、役員、職員、任期付職員、ワイドキャリアスタッフ職員、再任用職員、再雇用職員をいう。

二　「利用者」とは、役職員以外の産技研を利用するすべての者をいう。

三　「情報資産」とは、次にあげるものをいう。

イ　情報　役職員や利用者が産技研の業務上作成し、収集し、又は取得した JIS X 1009 に定める情報であって、ハードウェア又は記憶装置に保存又は蓄積されているもの及び書類に記録されたもの

ロ　情報システム　JIS X 1009 に定めるハードウェア、ソフトウエア、ネットワーク及び記憶装置で構成されるものであって、これら全体で情報を管理し業務処理を行うもの

四　「情報セキュリティ」とは、情報資産が備えるべき次に掲げる性質を健全に保つことをいう。

イ　機密性（権限を持つ者だけがアクセスできること。以下同じ。）

ロ　完全性（情報及びその処理方法の正確さ並びに完全さが保護されていること。以下同じ。）

ハ　可用性（許可された利用者が必要なときに情報及び情報システムへアクセスすることが保証されていること。以下同じ。）

五　「情報セキュリティポリシー」とは、情報セキュリティ基本方針及び本規程をあわせたものをいう。

六　「情報セキュリティの侵害」とは、情報の流失、漏洩、改ざん、破壊、障害等により情報資産が侵害されることをいう。

（対象の範囲）
第３条　本規程は、産技研に適用される。
２　情報資産の範囲
本規程が対象とする情報資産は、次のとおりとする。
一　産技研における産業技術に関する支援業務（試験・研究、普及及び技術支援等）に関する情報及びそれに関する情報
二　産技研の所有する知的財産及びそれに関する情報
三　施設、設備機器及び情報システムに関する契約文書、取扱説明書、使用許諾証明書
四　その他産技研の運営に必要な文書などの情報

第２章　組織体制

（最高情報セキュリティ責任）
第４条　理事長は、最高情報セキュリティ責任者を置かなければならない。
２　最高情報セキュリティ責任者は、理事の中から１名、理事長が指名する。
３　最高情報セキュリティ責任者は、産技研における全ての情報資産の管理及び情報セキュリティ対策に関する最終決定権限及び責任を有する。

（情報セキュリティ責任者）
第５条　最高情報セキュリティ責任者は、最高情報セキュリティ責任者を補佐するために情報セキュリティ責任者を置くことができる。
２　情報セキュリティ責任者は、部長職にある者の中から最高情報セキュリティ責任者が指名する。
３　情報セキュリティ責任者は、産技研の全ての情報資産の管理に関する権限及び責任を有する。
４　情報セキュリティ責任者は、情報セキュリティ管理者及び情報システム管理者の所管する情報資産とその管理責任を明示しなければならない。
５　情報セキュリティ責任者は、情報セキュリティ管理者と情報システム管理者に対して、情報セキュリティに関する指導及び助言を行う権限を有する。
６　情報セキュリティ責任者は、産技研の情報資産に対する侵害が発生した場合又は侵害のおそれがある場合に、最高情報セキュリティ責任者の指示に従い、最高情報セキュリティ責任者が不在の場合には自らの判断に基づき、必要かつ十分な措置を行う権限及び責任を有する。
７　情報セキュリティ責任者は、情報資産に関する情報セキュリティ実施手順の維持・管理を行う権限及び責任を有する。
８　情報セキュリティ責任者は、緊急時等の円滑な情報共有を図るため、連絡体制を整備しなければならない。

９　情報セキュリティ責任者は、情報セキュリティポリシーの遵守に関する意見の集約及び役職員に対する教育、訓練、助言及び指示を行う。

（情報セキュリティ管理者）

第６条　最高情報セキュリティ責任者は、情報セキュリティ管理者を置かなければならない。

２　情報セキュリティ管理者は、室長、支所長、グループ長、チームリーダ、課長をもってあてる。

３　情報セキュリティ管理者はその所管する室、支所、グループ、チーム、課（以下「課室等」）の情報セキュリティ対策に関する権限及び責任を有する。

４　情報セキュリティ管理者は、所管する情報資産に係る情報セキュリティ実施手順の維持・管理を行う。

５　情報セキュリティ管理者は、その所掌する課室等において、情報資産に対する侵害が発生した場合又は侵害のおそれがある場合には、情報セキュリティ責任者へ速やかに報告を行い、指示を仰がなければならない。

　ただし、情報セキュリティ責任者が不在の場合は、最高情報セキュリティ責任者へ速やかに報告を行い、指示を仰ぐ。

（情報システム管理者）

第７条　最高情報セキュリティ責任者は、情報システムごとに情報システム管理者を置かなければならない。

２　情報システム管理者は、所管する情報システムにおける情報セキュリティに関する権限及び責任を有する。

３　情報システム管理者は、所管する情報システムに係る情報セキュリティ実施手順の維持・管理を行う。

４　情報システム管理者は、その所掌する課室等において、情報システムに対する侵害が発生した場合又は侵害のおそれがある場合には、情報セキュリティ責任者へ速やかに報告を行い、指示を仰がなければならない。

　ただし、情報セキュリティ責任者が不在の場合は、最高情報セキュリティ責任者へ速やかに報告を行い、指示を仰ぐ。

（情報システム担当部門）

第８条　情報システム管理者の指示等に従い、情報システムの開発、設定の変更、運用、更新等の作業を行う者を、情報システム担当部門とする。

（情報資産管理委員会）

第９条　最高情報セキュリティ責任者は、産技研の情報セキュリティ対策を統一的に行うため、情報資産管理委員会を置かなければならない。

２　情報資産管理委員会に委員長を１人置く。

３　委員長は、部長職にある者の中から最高情報セキュリティ責任者が指名する。

４　委員長は、最高情報セキュリティ責任者、情報セキュリティ責任者、情報セキュリティ管理者、情報システム管理者を兼ねることはできない。

５　情報資産管理委員会は、次にあげる情報セキュリティに関する重要な事項について最高情報セキュリティ責任者に報告あるいは提言を行う。

一　情報セキュリティ基本方針の改訂に関すること

二　情報セキュリティ規程の改訂に関すること

三　情報資産の分類基準に関すること

四　関連する規程に関すること

五　情報セキュリティの事故、障害についての調査、分析に関すること

六　情報システムの導入・開発についての計画に関すること

七　情報セキュリティについての監査、自己点検に関すること

八　その他、最高情報セキュリティ責任者が定めたこと

６　情報資産管理委員会は、毎年度、産技研における情報セキュリティ対策の改善計画案を策定し、最高情報セキュリティ責任者へ提出しなければならない。

（兼務の禁止）

第１０条　情報セキュリティ対策の実施において、やむを得ない場合を除き、承認又は許可の申請を行う者とその承認者又は許可者は、同じ者が兼務してはならない。

第３章　情報資産の分類と管理方法

（情報資産の分類）

第１１条　情報セキュリティ責任者は、情報資産について、表１、表２、表３に定める機密性、完全性及び可用性に関する基準に従い分類し、取り扱いについて管理方法を定め、必要に応じ取り扱いの制限を行う。

表１　機密性による情報資産の分類

分類	分類基準
機密性３	業務で取り扱う情報資産のうち、秘密文書に相当する機密性を要する情報資産 例）お客様が特定される危険がある情報資産 例）お客様がからお預かりした情報資産 　依頼試験、技術相談、受託研究、共同研究、技術審査など 例）公表前の研究、開発、調査、入札に関するもの中で、目的や内容が特定される危険がある情報資産 　研究、調査、知財、契約他 例）その他、漏洩すると業務に支障が生じる情報資産 　広報の一部、他
機密性２	業務で取り扱う情報資産のうち、秘密文書に相当する機密性は要しないが、直ちに一般に公表することを前提としていない情報資産 例）一般の文書、広報の一部、他
機密性１	機密性２、３の情報資産以外の情報資産 例）公表後の広報、他

表２　完全性による情報資産の分類

分類	分類基準
完全性２	業務で取り扱う情報資産のうち、改ざん、誤びゅう又は破損により、業務の適確な遂行に支障を及ぼすおそれがある情報資産 例）規定類、情報システムの一部、他
完全性１	完全性２の情報資産以外の情報資産 例）情報システムの一部、他

表３　可用性による情報資産の分類

分類	分類基準
可用性２	業務で取り扱う情報資産のうち、滅失、紛失又は当該情報資産が利用不可能であることにより、業務の安定的な遂行に支障を及ぼすおそれがある情報資産 例）規定類 例）情報システムの一部 　外向け Web サーバ、メールサーバ 　各種アプリケーション（庶務・文書・財務・決議・薬品・業務系システム） 　産技研情報ネットワーク（冗長化）　など
可用性１	可用性２の情報資産以外の情報資産 例）情報システムの一部、他

（情報資産の管理）

第１２条　情報セキュリティ管理者及び情報システム管理者は、その所管する情報資産について管理責任を有する。

　また、情報資産が複製又は伝送された場合には、複製等された情報資産も第１１条の分類に基づき管理しなければならない。

２　情報資産を取り扱う者は、情報資産の分類に応じ、適切な取り扱いをしなければならない。

３　情報資産を取得した者あるいは作成した者は、取得した情報資産の分類が不明な場合、情報セキュリティ管理者に判断を仰がなければならない。

４　役職員は、業務上必要のない情報を取り扱ってはならない。

５　情報資産を取り扱う者は、情報資産の分類が異なる情報が複数記録されている場合、最高度の分類に従って取り扱わなければならない。

（物理的セキュリティの適切な管理）

第１３条　情報セキュリティ責任者は、産技研のすべての情報資産を適切に管理するため、物理的セキュリティの管理方法を定める。

　定める項目は次のとおりである。

一　管理区域の管理

二　情報資産を取り扱うために必要な設備の管理

２　情報セキュリティ管理者、情報システム管理者は、前項で定める管理方法に基づき、その所管する情報資産に関する物理的セキュリティを適切に管理しなければならない。

（人的セキュリティの適切な管理）

第１４条　情報セキュリティ責任者は、産技研のすべての情報資産を適切に管理するため、人的セキュリティの管理方法を定める。

　定める項目は次のとおりである。

一　役職員の遵守事項

二　研修・訓練

三　事故、欠陥等の報告

四　身分証明書及びパスワード等の管理

２　情報セキュリティ管理者、情報システム管理者は、前項で定める管理方法に基づき、その所管する情報資産に関する人的セキュリティを適切に管理しなければならない。

（役職員の遵守事項）

第１５条　役職員は、情報セキュリティポリシー及び実施手順（以下「情報セキュリティポリシー等」）を遵守しなければならない。また、情報セキュリティ対策について不明な点、遵守することが困難な点等がある場合は、速やかに所属の情報セキュリティ管理者に相談し、指示を仰がなければならない。

２　役職員は、異動、退職等により業務を離れる場合には、利用していた情報資産を、返却しなければならない。また、その後も業務上知り得た情報を漏らしてはならない。

（契約職員及び臨時職員への対応）

第１６条　情報セキュリティ管理者は、契約職員及び臨時職員に対し、採用時に情報セキュリティポリシー等について、必要な内容を理解させ、実施及び遵守させなければならない。

２　情報セキュリティ管理者は、契約職員及び臨時職員の採用の際、必要に応じ、情報セキュリティポリシー等を遵守する旨の同意書への署名を求める。

３　情報セキュリティ管理者は、契約職員及び臨時職員に情報資産を取り扱う作業を行わせる場合において、情報資産の使用は必要最低限の範囲としなければならない。

（情報セキュリティポリシー等の掲示）

第１７条　情報セキュリティ管理者は、役職員が常に情報セキュリティポリシー等を閲覧できるように掲示しなければならない。

（外部委託事業者への対応）

第１８条　情報セキュリティ管理者は、情報資産を取り扱う業務を外部委託事業者に発注する場合、外部委託事業者から再委託を受ける事業者も含めて、情報セキュリティポリシー等について、必要な内容を理解させ、実施及び遵守させなければならない。

（情報セキュリティに関する研修・訓練）

第１９条　最高情報セキュリティ責任者は、定期的に情報セキュリティに関する研修・訓練を実施しなければならない。

（研修計画の立案及び実施）

第２０条　最高情報セキュリティ責任者は、すべての役職員を対象とする情報セキュリティに関する研修計画を立案し、毎年度最低１回受講させなければならない。

２　新規採用の役職員を対象とする情報セキュリティに関する研修を実施しなければならない。

３　研修は、情報セキュリティ責任者、情報セキュリティ管理者、情報システム管理者、その他役職員に応じたものにしなければならない。

４　最高情報セキュリティ責任者は、毎年度１回、情報資産管理委員会に対して、役職員の情報セキュリティ研修の実施状況について報告しなければならない。

（緊急時対応訓練）

第２１条　最高情報セキュリティ責任者は、緊急時対応を想定した訓練を定期的に実施しなければならない。訓練計画は、ネットワーク及び情報システムの規模等を考慮し、訓練実施の範囲等を定め、また、効果的に実施できるようにしなければならない。

（研修・訓練への参加）

第２２条　常勤、非常勤を含めたすべての役職員は、定められた研修・訓練に参加しなければならない。

（事故、欠陥等の報告）

第２３条　役職員は、情報セキュリティに関する事故、欠陥等を発見した場合、速やかに所属の情報セキュリティ管理者に報告しなければならない。

２　情報セキュリティ管理者は、報告のあった事故、欠陥等について、必要に応じて情報セキュリティ責任者に報告しなければならない。

３　情報セキュリティ責任者は、最高情報セキュリティ責任者に報告しなければならない。また、情報セキュリティ責任者は当該事故、欠陥等が情報システムに関連する場合、速やかに情報システム管理者に報告しなければならない。

４　最高情報セキュリティ責任者は、情報システム等の情報資産に関する事故、欠陥等について、外部から報告を受けるための窓口を設置し、当該窓口への連絡手段を公表しなければならない。

（事故、欠陥等の分析・記録等）

第２４条　情報セキュリティ責任者は、事故、欠陥等を引き起こした部門の情報セキュリティ管理者及び情報システム管理者と連携し、これらの事故、欠陥等を分析し、記録を保存し、結果を最高情報セキュリティ責任者に報告なければならない。

（身分証明書等の取り扱い）

第２５条　最高情報セキュリティ責任者は、役職員に身分証明書等を与えなければならない。

２　役職員は、自己の管理する身分証明書等に関し、次の事項を遵守しなければならない。

一　退職時には、身分証明書等を情報セキュリティ責任者へ返却しなければならない。

二　身分証明書等を紛失した場合には、速やかに情報セキュリティ責任者に通報し、指示に従わなければならない。

３　情報セキュリティ責任者は、身分証明書等を回収した場合には、適切な廃棄しなければならない。

（ユーザアカウントの取り扱い）

第２６条　役職員は、自己の管理するユーザアカウントに関し、次の各号の事項を遵守しなければならない。

一　自己が利用しているユーザアカウントは、他人に利用させてはならない。

二　共用ユーザアカウントを利用する場合は、共用ユーザアカウントの利用者以外に利用させてはならない。

（パスワードの取り扱い）

第２７条　役職員は、自己の管理するパスワードに関し、適切に管理しなければならない。

（技術的セキュリティ）

第２８条　情報セキュリティ責任者は、産技研のすべての情報資産を適切に管理するため、技術的セキュリティの管理方法を定める。

定める管理方法の項目は次のとおりである。

一　ハードウェアの導入・調達・保守・管理

二　ネットワークの維持・管理

三　情報システム及び情報サービスの導入・調達・開発・管理

四　セキュリティ侵害対策・違反防護策等の導入・維持・管理

なお、各項目の細目については、別途運用管理基準等にこれを定める。

２　情報セキュリティ管理者、情報システム管理者は、前項で定める管理方法に基づき、その所管する情報資産に関する技術的セキュリティを適切に管理しなければならない。

第４章　情報セキュリティポリシー等の遵守状況の確認

（遵守状況の確認及び対処）

第２９条　情報セキュリティ責任者は、情報セキュリティポリシー等の遵守状況について確認を行い、問題を認めた場合には、速やかに最高情報セキュリティ責任者に報告しなければならない。

２　最高情報セキュリティ責任者は、発生した問題について、適切かつ速やかに対処しなければならない。

（情報資産の取扱状況調査）

第３０条　最高情報セキュリティ責任者は、不正な取り扱いの調査のために、役職員が使用している書棚等の什器類、パソコン等の端末、記録媒体のアクセス記録、電子メールの送受信記録等の利用状況を調査することができる。

２　前項の調査は、最高情報セキュリティ責任者が指名した者に行わせることができる。

３　前項の調査を行う場合には、最高情報セキュリティ責任者はあらかじめ情報資産管理委員会へ調査の目的、時期、方法及び結果の報告の方法について諮問しなければならない。

４　第１項の調査を行った場合には、最高情報セキュリティ責任者はその結果を情報資産管理委員会に報告しなければならない。また、調査を行ったことを調査の対象となった役職員に報告しなければならない。

（役職員の報告義務）

第３１条　役職員は、情報セキュリティポリシー等に対する違反行為を発見した場合、直ちに所属の情報セキュリティ管理者に報告を行わなければならない。

２　報告を受けた情報セキュリティ管理者は、その内容を情報セキュリティ責任者に報告しなければならない。

３　違反行為が直ちに情報セキュリティ上重大な影響を及ぼす可能性があると情報セキュリティ責任者が判断した場合は、緊急時対応計画に従って適切に対処しなければならない。

第５章　侵害時の対応

（緊急時対応計画の策定）

第３２条　最高情報セキュリティ責任者は、情報セキュリティに関する事故、情報セキュリティポリシー等の違反等により情報資産への侵害が発生した場合又は発生するおそれがある場合において連絡、証拠保全、被害拡大の防止、復旧、再発防止等の措置を迅速かつ適切に実施するために、緊急時対応計画を定めておかなければならない。

（緊急時対応計画に盛り込むべき内容）

第３３条　緊急時対応計画には、以下の内容を定めなければならない。

一　関係者の連絡先

二　発生した事案に係る報告すべき事項

三　発生した事案への対応措置

四　再発防止措置の策定

（事業継続計画との整合性確保）

第３４条　産技研が自然災害等に備えて危機管理の計画を整備する場合、最高情報セキュリティ責任者は当該計画と情報セキュリティポリシー等の整合性を確保しなければならない。

（緊急時対応計画の見直し）

第３５条　情報資産管理委員会は、情報セキュリティを取り巻く状況の変化や組織体制の変動等に応じ、必要に応じて緊急時対応計画の規定を見直さなければならない。

（例外措置の許可）

第３６条　情報セキュリティ管理者及び情報システム管理者は、情報セキュリティに関する規定を遵守することが困難な状況で、業務の適正な遂行を継続するため、遵守事項とは異なる方法を採用し、又は遵守事項を実施しないこと（以下「例外措置」）について合理的な理由がある場合には、情報セキュリティ責任者に許可を求めることができる。

２　情報セキュリティ責任者は、情報セキュリティ管理者あるいは情報システム管理者から例外措置の許可の求めがあった場合、最高情報セキュリティ責任者の許可を得て、例外措置を許可することができる。

３　最高情報セキュリティ責任者及び情報セキュリティ責任者は、例外措置について必要に応じて適切な措置を行わなければならない。

（緊急時の例外措置）

第３７条　情報セキュリティ管理者及び情報システム管理者は、業務の遂行に緊急を要する等の場合であって、例外措置を実施することが不可避のときは、事後速やかに情報セキュリティ責任者に報告しなければならない。

２　情報セキュリティ責任者は、例外措置を緊急に実施したことについて、情報セキュリティ管理者及び情報システム管理者から事後に連絡があった場合、その旨を最高情報セキュリティ責任者に報告しなければならない。

３　最高情報セキュリティ責任者及び情報セキュリティ責任者は、緊急に行われた例外措置について、必要に応じて適切な措置を行わなければならない。

（例外措置の申請書等の管理）

第３８条　最高情報セキュリティ責任者は、例外措置の申請書及び審査結果を適切に保管しなければならない。

第６章　外部委託

（外部委託先の選定基準）

第３９条　情報セキュリティ管理者は、外部委託先の選定にあたり、委託内容に応じた情報セキュリティ対策が確保されることを確認しなければならない。

２　情報セキュリティ管理者は、情報セキュリティマネジメントシステムの国際規格の認証取得状況等を参考にして、事業者を選定しなければならない。

（契約項目）

第４０条　情報システムの運用等を外部委託する場合には、委託事業者との間で必要に応じて次の各号の情報セキュリティ要件を明記した契約を締結しなければならない。

一　情報セキュリティポリシー等に関する規定の遵守

二　委託先の責任者、委託内容、作業者、作業場所の特定

三　提供されるサービスレベルの保証

四　従業員に対する教育の実施

五　提供された情報の目的外利用及び受託者以外の者への提供の禁止

六　業務上知り得た情報の守秘義務

七　再委託に関する制限事項の遵守

八　委託業務終了時の情報資産の返還、廃棄等

九　委託業務の定期報告及び緊急時報告義務

十　産技研による監査、検査

十一　産技研による事故時等の公表

十二　情報セキュリティポリシー等が遵守されなかった場合の規定（損害賠償等）

（確認・措置等）

第４１条　情報セキュリティ管理者は、外部委託事業者において必要なセキュリティ対策が確保されていることを定期的に確認し、必要に応じ、前条の契約に基づき措置しなければならない。また、その内容を情報セキュリティ責任者に報告しなければならない。

２　情報セキュリティ責任者は、報告に対して適切な措置を行わなければならない。また、その重要度に応じて最高情報セキュリティ責任者に報告しなければならない。

３　最高情報セキュリティ責任者は、報告に対して適切な措置を行わなければならない。

第７章　法令遵守

（法令遵守）

第４２条　役職員は、職務の遂行において使用する情報資産を保護するために、次の各号の法令のほか関係法令を遵守し、これに従わなければならない。

一　地方独立行政法人法（平成１５年7月１６日法律１０８号）

二　著作権法（昭和４５年5月6日法律４８号）

三　不正アクセス行為の禁止等に関する法律（平成１１年8月１３日法律１２８号）

四　個人情報の保護に関する法律（平成１５年5月３０日法律５７号）

五　東京都個人情報保護条例（平成２年１２月２１日条例１１３号）

第８章　違反時の対応等

（懲戒処分）

第４３条　情報セキュリティポリシー等に違反した役職員及びその監督責任者は、その重大性、発生した事案の状況等に応じて、就業規則等による懲戒処分の対象とする。

（違反時の対応）

第４４条　役職員の情報セキュリティポリシー等に違反する行動を確認した場合には、速やかに次の措置を講じなければならない。

一　情報セキュリティ責任者は違反を確認した場合、当該役職員が所属する課室等の情報セキュリティ管理者に通知し、適切な措置を求めなければならない。

二　情報システム管理者が違反を確認した場合、違反を確認した者は速やかに情報セキュリティ責任者及び当該役職員が所属する課室等の情報セキュリティ管理者に通知し、適切な措置を求めなければならない。

三　情報セキュリティ管理者の指導によっても改善されない場合、情報セキュリティ責任者は、当該役職員の情報資産の取り扱いを停止するなど、適切な措置を行うことができる。その後速やかに、情報セキュリティ責任者は、役職員の権利を停止あるいは剥奪した旨を最高情報セキュリティ責任者及び当該役職員が所属する課室等の情報セキュリティ管理者に通知しなければならない。

第９章　評価・見直し

（監査の実施方法）

第４５条　情報資産管理委員会は、情報セキュリティ監査人を指名し、情報資産における情報セキュリティ対策状況について、定期的に又は必要に応じて監査を行わせなければならない。

（監査補助者）

第４６条　情報セキュリティ監査人は、監査を行うために監査補助者を置くことができる。

（監査実施計画の立案及び実施への協力）

第４７条　情報セキュリティ監査人は、監査を行うに当たって、監査実施計画を立案し、情報資産管理委員会の承認を得なければならない。

２　監査を受ける役職員は、監査の実施に協力しなければならない。

（外部委託事業者に対する監査）

第４８条　外部委託事業者に委託している場合、情報セキュリティ監査人は外部委託事業者から受託している事業者も含めて、情報セキュリティポリシー等の遵守について監査を定期的に又は必要に応じて行わなければならない。

（監査の報告）

第４９条　情報セキュリティ監査人は、監査結果を取りまとめ、情報資産管理委員会に報告しなければならない。

２　情報資産管理委員会は、監査結果の報告に意見を付して、最高情報セキュリティ責任者に報告しなければならない。

（監査に関する文書の保管）

第５０条　情報セキュリティ監査人は、監査の実施を通して収集した監査証拠、監査報告書の作成のための監査調書など監査に関する文書を、紛失等が発生しないように適切に保管しなければならない。

（監査結果への対応）

第５１条　最高情報セキュリティ責任者は、監査結果を踏まえ、情報セキュリティ責任者に対し、当該事項への対処を指示しなければならない。

２　情報資産管理委員会は、監査結果を情報セキュリティポリシー等の見直し、その他情報セキュリティ対策の見直し時に活用しなければならない。

（自己点検の実施方法）
第５２条　情報セキュリティ責任者は、情報セキュリティポリシー等に沿った情報セキュリティ対策状況について、毎年度又は必要に応じて自己点検を行わなければならない。
２　情報セキュリティ責任者は、自己点検の指針を策定し、役職員に周知しなければならない。

（自己点検の報告）
第５３条　情報セキュリティ管理者及び情報システム管理者は、所管する情報資産について自己点検を実施し、情報セキュリティ責任者に報告しなければならない。
２　情報セキュリティ責任者は、自己点検結果とそれに基づく改善策を取りまとめ、最高情報セキュリティ責任者に報告しなければならない。
３　最高情報セキュリティ責任者は、自己点検結果とそれに基づく改善策を、情報資産管理委員会に報告しなければならない。

（自己点検結果の活用）
第５４条　役職員は、自己点検の結果に基づき、自己の権限の範囲内で改善を図らなければならない。
２　最高情報セキュリティ責任者は、この点検結果を情報セキュリティポリシー等の見直し、その他情報セキュリティ対策の見直し時に活用しなければならない。

（情報セキュリティポリシー等の見直し）
第５５条　情報資産管理委員会は、情報セキュリティポリシー等について監査及び自己点検の結果並びに情報セキュリティに関する状況の変化等をふまえ、必要があると認めた場合、その見直しを行う。

附則
（施行期日）
１　この規程は、平成１９年3月２６日から施行する。